Between Both Worlds
4 years of a joint PhD

Moritz Müller| NetSys PhD Forum

16 September 2021

SIDN LABS

2017: Where it all began

2017: PhD! But how and where?

2017: Let's get started!

SDN LABS

2017: The long and winding road to the Root Rollover paper

SIDN LABS

2017: The long and winding road to the Root Rollover paper

SIDN LABS

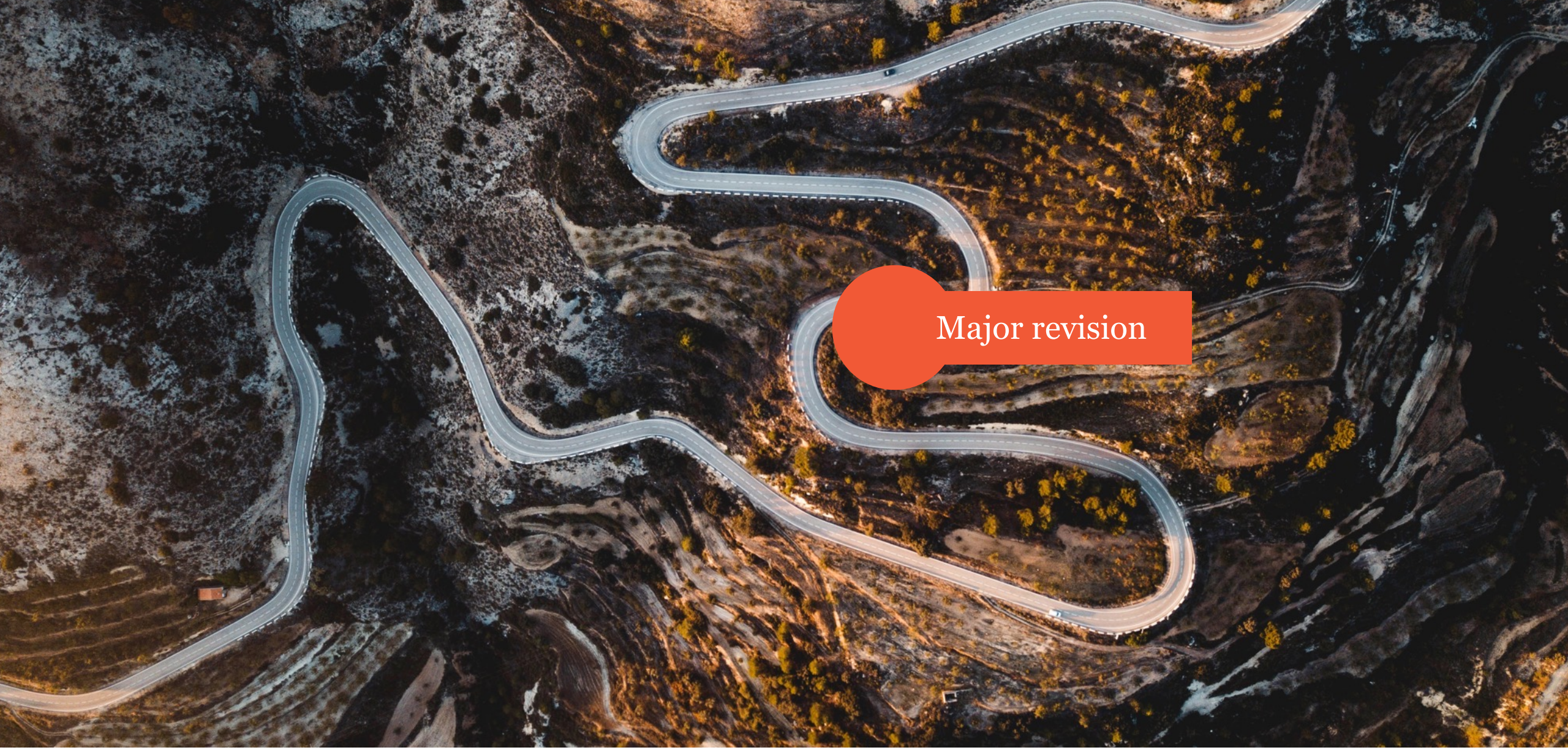
2017: The long and winding road to the Root Rollover paper

SIDN LABS

2017: The long and winding road to the Root Rollover paper

2018: The long and winding road to the Root Rollover paper

SIDN LABS



2019: The long and winding road to the Root Rollover paper

SIDN LABS

2019: The long and winding road to the Root Rollover paper

SIDN LABS

2018: A few steps back on the road to the Root Rollover paper

SIDN LABS

Working in a team

SIDN LABS

2019: Finally arrived

2020

SDN LABS

Photo by Drew Coffman

2020

SDN LABS

2020: DNSSEC it is

The Reality of Algorithm Agility: Studying the DNSSEC Algorithm Life-Cycle

Moritz Müller
SIDN Labs and University of Twente

Willem Toorop
NLnet Labs

Jelte Jansen
SIDN Labs

Roland van Rijswijk-Deij
University of Twente and NLnet Labs

Taejoong Chung
Virginia Tech

ABSTRACT

The DNS Security Extensions (DNSSEC) add data origin authentication and data integrity to the Domain Name System (DNS), the naming system of the Internet. With DNSSEC, signatures are added to the information provided in the DNS using public key cryptography. Advances in both cryptography and cryptanalysis make it necessary to deploy new algorithms in DNSSEC, as well as deprecate those with weakened security. If this process is *easy*, then the protocol has achieved what the IETF terms "*algorithm agility*". In this paper, we study the lifetime of algorithms for DNSSEC. This includes: (i) standardizing the algorithm, (ii) implementing support in DNS software, (iii) deploying new algorithms at domains and recursive resolvers, and (iv) replacing deprecated algorithms. Using data from more than 6.7 million signed domains and over 10,000 vantage points in the DNS, combined with qualitative studies, we show that DNSSEC has only partially achieved algorithm agility. Standardizing new algorithms and deprecating insecure ones can take years. We highlight the main barriers for getting new algorithms deployed, but also discuss success factors. This study provides key insights to take into account when new algorithms are introduced, for example when the Internet must transition to quantum-safe public key cryptography.

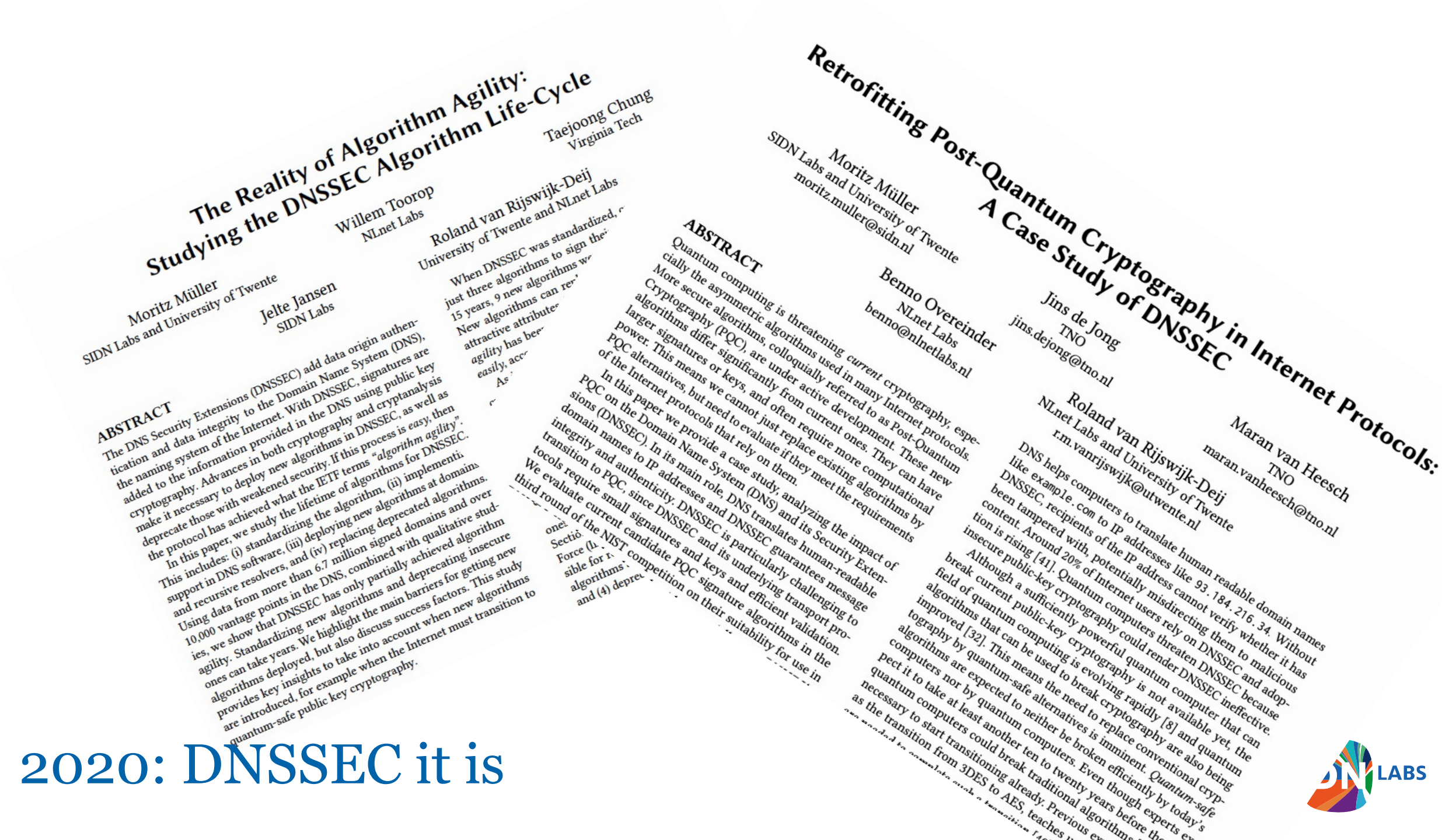
When DNSSEC was standardized, operators had the choice of just three algorithms to sign their domains with. Over the past 15 years, 9 new algorithms were added and 5 were deprecated [69]. New algorithms can replace insecure algorithms, or have more attractive attributes, like smaller keys and signatures. *Algorithm agility* has been achieved, if this replacement can be carried out *easily*, according to RFC 7696 [27].

As in other Internet protocols, algorithm agility in DNSSEC is crucial, because we do not know how fast attacks on cryptographic algorithms evolve, only that, at some point, algorithms will be broken [27]. This becomes even more urgent with the rise of quantum computers [8]. Even though it is still not clear, *when* quantum computers will become generally available, they do have the potential to break *all* current algorithms used in DNSSEC. Then, it becomes crucial to replace vulnerable algorithms by *quantum-safe* algorithms easily and fast.

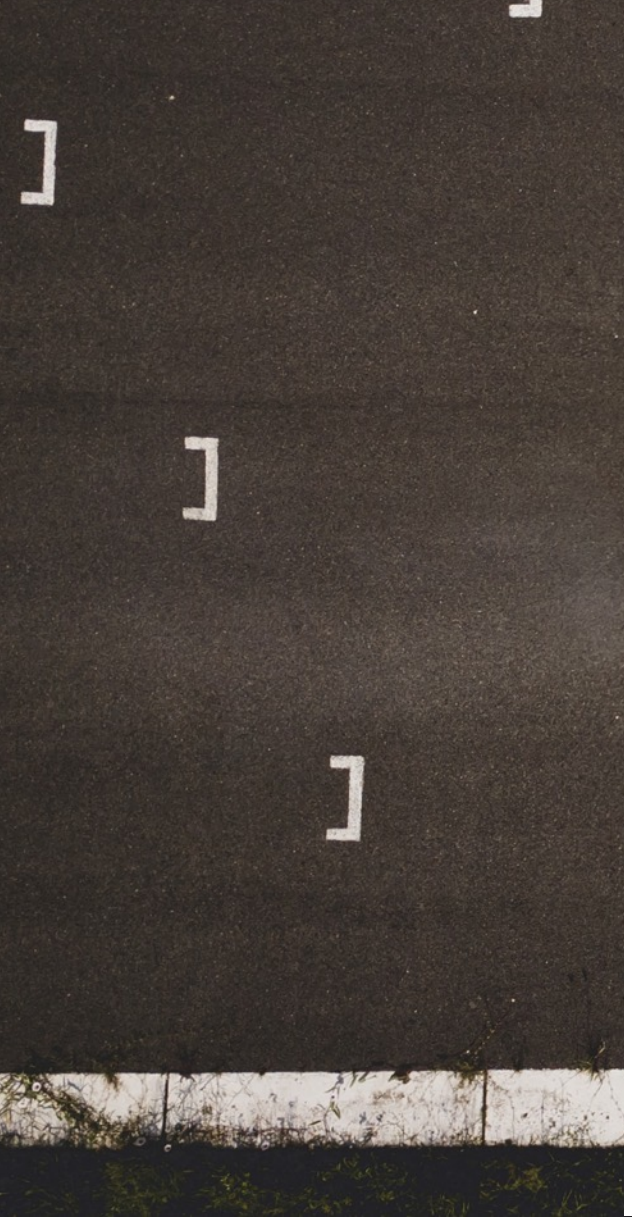
In DNSSEC, introducing new algorithms and replacing existing ones is a four-stage process and we explain it in more detail in Section 2.2: (1) standardization at the Internet Engineering Task Force (IETF), (2) implementation in software and at entities responsible for registering and publishing domain names, (3) deploying algorithms at domain names and rolling out validating resolvers, and (4) deprecating insecure algorithms.

2020: DNSSEC it is

SIDN LABS



2020: DNSSEC it is



Wrapping things up

Wrapping things up

Photo by Anton Shuvalov

Wrapping things up

Moritz Müller
moritz.muller@sidn.nl
sidnlabs.nl

Questions? Comments?